SYSTEM AND METHOD OF SENDING AND RECEIVING SECURE DATA WITH A SHARED KEY

Lynn D. Spraggs

BACKGROUND OF THE INVENTION

1. Field of the invention

The present invention relates generally to computer security and more specifically to allow the secure transfer and receipt of data between computers.

2. Description of the Prior Art

In order to securely transfer data between computers on the Internet, various different types of encryption/decryption methods are used. One way of securely transferring data over the Internet includes the use of a public key/private key system.

A public key is provided by some designated authority as a key that, combined with a private key derived from the public key, can be used to effectively encrypt and decrypt messages and digital signatures.

In public key cryptography, a public and private key are created simultaneously using the same algorithm (a popular one is known as

RSA) by a certificate authority. The private key is given only to the requesting party and the public key is made publicly available (as part of a digital certificate) in a directory that all parties can access. The private key is never shared with anyone or sent across the Internet. The private key is used to decrypt text that has been encrypted with the public key counterpart by someone else who has the public key.

Public key cryptography generally requires a large mathematical decomposition in order to work effectively. Generally, the length of a private key is in the order of 64 bytes. Decomposing these relatively small private keys requires considerable computational power. Public key cryptography is generally used as a one-way encryption and if a private key is changed, then everyone else that has the public key counterpart must receive a new public key.

Thus, it would be desirable to provide a system and method of securing data that is easy to use, does not require a public/private key, allows for a larger private key for more security, uses less computation power than public key cryptography, and can be used in two directions.

SUMMARY OF THE INVENTION

A system and method is provided for sending and receiving secure data. The data is secured by encrypting and decrypting the data with a key that is shared between authorized users and the server computer. As the server computer receives a user's encrypted data, the server computer decrypts the data using the user's shared key stored in a database on the server. The server computer can then process the data according to the user's instructions, this could include securely storing the data for retrieval by another user, processing the data, and/or securely sending the data to a second user by encrypting the data with the second user's shared key.

BRIEF DESCRIPTION OF THE DRAWINGS

The present invention may be better understood, and its numerous objects, features, and advantages made apparent to those skilled in the art by referencing the accompanying illustrations. For simplicity and ease of understanding, common numbering of elements is employed where an element is the same in different illustrations.

FIG. 1 is a schematic diagram illustrating a sending client transmitting secure data through a server to a receiving client over the Internet, in accordance with the present invention;

FIG. 2 is a block diagram of the server computer shown in FIG. 1, in accordance with the present invention;

FIG. 3 is a block diagram of one embodiment of the non-volatile memory module located within the server computer of FIG. 2; and

FIG. 4 is a block diagram of the client computers shown in FIG. 1, in accordance with the present invention;

FIG. 5 is a block diagram of one embodiment of the non-volatile memory module located within the client computers of FIG. 4;

FIG. 6 is a flowchart of a method illustrating how a sending client, having a shared private key, passes encrypted data to a server computer, according to the invention;

FIG. 7 is a flowchart of a method illustrating how a receiving client, having a shared private key, requests secure data from a server computer, in accordance with the invention; and

FIG. 8 is a flowchart of a method illustrating how a client, having a shared private key, passes secure data through a server computer.

DETAILED DESCRIPTION OF THE INVENTION

The following is a detailed description of illustrative embodiments of the present invention. As these embodiments of the present invention are described with reference to the aforementioned illustrations, various modifications or adaptations of the methods and or specific structures described may become apparent to those skilled in the art. All such modifications, adaptations, or variations that rely upon the teachings of the present invention, and through which these teachings have advanced the art, are considered to be within the spirit and scope of the present invention. Hence, these descriptions and drawings should not be considered in a limiting sense, as it is understood that the present invention is in no way limited to only the embodiments illustrated.

Referring now to FIG. 1, a schematic diagram illustrates a server 100 used to receive encrypted data from a sending client computer 102 and transmit encrypted data to a receiving client computer 104 through the Internet 106 using shared private keys. The sending client 102 and receiving client 104 share their own private key with the server 100, but do not share their private key with anyone else.

FIG. 2 is a block diagram of the server computer 100 shown in FIG. 1. Server 100 includes a CPU 202, a RAM 204, a non-volatile

memory 206, an input device 208, a display 210, and an Internet interface 212 for providing access to the Internet.

FIG. 3 is a block diagram of one embodiment of the non-volatile memory module 206 located within the server computer 100 of FIG. 2. The non-volatile memory 206 includes a private server key 302, a database of user private keys 304, an encrypt/decrypt engine 306, a web server engine 308 containing web page forms 310, and a secure data database 312 for storing encrypted data. The private server key 302 is known only to the server and is not shared with anyone. The database of user private keys 304 includes the private keys of registered users. Each private key of a registered user is shared only with the server and not with other users.

The encrypt/decrypt engine 306 is programmed to encrypt and decrypt data using a password or a key. Excellent results can be obtained when using the blowfish algorithm for encryption and decryption. Other types of symmetric key encryption/decryption algorithms can also be employed within the encrypt/decrypt engine 306. The computation power required to encrypt and decrypt data using a single key is much less than the computational power required in a public/private key system, therefore longer keys can be used to provide an extremely high-level of security.

FIG. 4 is a block diagram of a sending client computer 102 or a receiving client computer 104 shown in FIG. 1. Client 102, 104 includes a CPU 402, a RAM 404, a non-volatile memory 406, an input device 408, a display 410, and an Internet interface 412 for providing access to the Internet.

FIG. 5 is a block diagram of one embodiment of the non-volatile memory module 404 located within the clients 102, 104 of FIG. 4. The non-volatile memory 406 includes an encrypt/decrypt engine 502 for encrypting and decrypting data. The encrypt/decrypt engine 502 can also be stored in RAM 404. Excellent results can be obtained when the encrypt/decrypt engine is served up as a Java™ applet to the clients 102, 104. The Java™ applet can be served up with a web page from an email sent to the clients 102, 104, and then stored on their hard drive.

FIG. 6 is a flowchart of a method illustrating how a sending client, with a shared private key, passes encrypted data to a server computer through the Internet in accordance with the invention. The process begins at step 600. The sending client establishes a session over the Internet with a suitable server by requesting a web page from the server computer at step 602. At step 604 the server sends a web page form from the web page forms database 310 to the sending client. Next at step 606 the sending client enters data into the web page along with the user's private key. At step 608 the data is encrypted with the

encrypt/decrypt engine at the sending client's computer using the user's private key and then sent to the server.

At step 610 the server receives the sending client's data and decrypts the data with the user's private key that is stored in the user private keys database 304. Then at step 612 the server re-encrypts the data using the server key 302. At step 614 the server stores the re-encrypted data in the secure data database 312 and at step 616 the process ends.

FIG. 7 is a flowchart of a method illustrating how a receiving client, having a shared private key, accesses encrypted data from the server computer through the Internet in accordance with the invention. The process begins at step 700. The receiving client establishes a session over the Internet with a suitable server by requesting the encrypted data from the server computer at step 702. At step 704 the server retrieves the encrypted data from the secure data database 312. At step 706 the server decrypts the data using the server key 302. Then at step 708 the server encrypts the data using the receiving client's private key that is stored in the user private keys database 304, and sends the encrypted data to the receiving client.

At step 710, the receiving client enters his private key, and at step 712 the encrypted data is decrypted with the receiving client's private key

using the encrypt/decrypt engine 502. At step 714 the receiving client can access or view the data, and at step 716 the process ends.

Sub D3

FIG. 8 is a flowchart of a method illustrating how a client, having a shared private key, passes secure data through a server computer over the Internet. This method is very similar to the process described in FIGS. 6 and 7. The process begins at step 800. A client having a private key shared with the server establishes a session over the Internet with the server by requesting a web page at step 802. At step 804 the server sends a web page form from the web page forms database 310 to the client. Next at step 806 the client enters data into the web page along with his private key shared with the server. At step 808 the data is encrypted with the encrypt/decrypt engine at the client's computer using the user's private key and then sent to the server.

At step 810 the server receives the sending client's data and decrypts the data with the user's private key that is stored in the user private keys database 304. Then at step 812 the server processes the data. This processing step can include many different types of applications including, but not limited to, storing data, calculating data, entering a stock transaction, verifying a credit card transaction, etc.

Sub D4

After the processing step is completed, at step 814 the server encrypts the processed data using the client's private key that is stored in the user private keys database 304 and sends the encrypted data to

the client. It is not necessary for the client to be the same client that began the process at step 802. The server can be used as an intermediary for passing and processing secure data between clients.

At step 816, the client receives the secure data and enters his private key. At step 818 the encrypted processed data is decrypted with the client's private key using the encrypt/decrypt engine 502. At step 820 the client can access or view the data, and at step 822 the process ends.

Various modifications can be made to the above described methods in order to provide a secure system and method of sending and receiving secure data with a shared key. This can be done in low-level and high-level security methods. For example, if a first user wanted to send a highly secure memo to a second person over the Internet using a screen-level encryption, the first user could write the memo at his computer, encrypt the memo and send it as an email through a server to the second user. The second user could then decrypt the email with his password and view the memo on his computer screen. The application used to decrypt and display the memo on the computer screen can be programmed so that the memo cannot ever be in a decrypted state in any file on the computer, including temporary files, but only programmed to display the decrypted memo on a computer screen. The application

could be resident on the user's computer, or it can be deployed as a Java™ applet.